This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-54. (Canceled)

55. (Currently Amended) A method of communicating between computers, comprising the steps of:

(1) transmitting from a first computer to an intermediate server computer a first HTTP POST message through a firewall ~~port~~ that is ~~normally~~ open to outbound Internet traffic, wherein the first HTTP POST message requests establishment of a connection between the first computer and the intermediate server computer over a first return path;

(2) receiving from the intermediate server computer a response including a connection identifier corresponding to the first return path;

(3) periodically transmitting from the intermediate server computer to the first computer a "keep alive" message over the first return path, if no further messages are sent to ~~received from~~ the first computer within a period of time;

(4) exchanging encryption keys between the first computer and the intermediate server computer;

(5) repeating steps (1) through (4) between a second computer and the intermediate server computer, thereby creating a second return path between the second computer and the intermediate server computer;

(6) transmitting encrypted information from the first computer through the firewall to the intermediate server computer using further HTTP POST messages ~~over the first return path~~; and

(7) transmitting the encrypted information from the intermediate server over the second return path.

56. (Previously Presented) The method of claim 55, further comprising the steps of, in the intermediate server computer, decrypting encrypted information received from the first computer using encryption keys shared between the first computer and the intermediate computer, and then re-encrypting the received information using encryption keys shared between the intermediate computer and the second computer.

57. (Currently Amended) A method of communicating between a first computer protected by a first firewall and a second computer protected by a different second firewall, comprising the steps of:

(1) at a third computer situated between the first firewall and the different second firewall, receiving a first HTTP message from the first computer through a ~~port in the~~ first firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic;

(2) from the third computer, sending a first response message to the first computer through the ~~port in the~~ first firewall, thereby establishing a first receive channel through the first firewall, wherein the first response message is linked to the first HTTP message;

(3) at the third computer, receiving a second HTTP message from the second computer through a ~~port in the~~ different second firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic;

(4) from the third computer, sending a second response message to the second computer through the ~~port in the different~~ second firewall, thereby establishing a second receive channel through the second firewall, wherein the second response message is linked to the second HTTP message;

(5) at the third computer, receiving a third encrypted HTTP message from the first computer through the ~~port in the~~ first firewall; determining that the third encrypted HTTP message is intended to be delivered to the second computer, and transmitting to the second computer the third encrypted HTTP message, wherein the third encrypted HTTP message is transmitted over the second receive channel through the second firewall to the second computer; and

(6) from the third computer, periodically transmitting "keep alive" messages to the first computer over the first receive channel and to the second computer ~~computers~~ over the second receive channel to avoid a time-out condition.

58. (Previously Presented) The method of claim 57, wherein step (5) is performed at the third computer by transmitting the third encrypted HTTP message to the second computer

without decrypting contents of the third encrypted HTTP message.

59. (Previously Presented) The method of claim 55, wherein at least one of the HTTP POST messages transmitted during step (6) comprises an identifier of said second computer encrypted with a first encryption key associated with the intermediate server, and wherein said encrypted information is encrypted with a second different encryption key associated with the second computer.

60. (Previously Presented) The method of claim 57, wherein the third encrypted HTTP message comprises:

an encrypted identifier of the second computer, the identifier encrypted with a first encryption key associated with the third computer, and

encrypted content for delivery to the second computer, the content encrypted with a different second encryption key associated with the second computer.

61. (New) The method of claim 56, wherein the encrypted information decrypted by the intermediate server computer comprises encrypted header information.

62. (New) The method of claim 61, wherein the encrypted header information comprises one or more of an encrypted IP address, an encrypted username of said second computer, an encrypted header length, an encrypted message length, an encrypted application identifier, an encrypted time and date stamp, and an encrypted message type.

63. (New) The method of claim 55, wherein communication between the first computer and the intermediate server computer is initiated by the first computer, and wherein communication between the second computer and the intermediate server computer is initiated by the second computer.

64. (New) The method of claim 55, wherein the first firewall and the second firewall are configured not to allow incoming network messages, unless the incoming network messages are responsive to network messages initiated by a computer inside the firewall.

65. (New) The method of claim 55, wherein periodically transmitting a "keep alive" message over the first return path comprises transmitting a "keep alive" message prior to a firewall timeout period to prevent the firewall from blocking traffic on the first receive path.

66. (New) A method of communicating between a first computer protected by a first firewall and a second computer protected by a different second firewall via a third intermediate computer, comprising the steps of:

receiving at the third intermediate computer a request transmitted from the second computer through the second firewall, wherein the request is to establish a receive channel between the second computer and the third intermediate computer;

transmitting from the third intermediate computer a response to the request, the response establishing a receive channel between the third intermediate computer and the second computer that is to be kept open for subsequent transmissions by the third intermediate computer;

receiving at the third intermediate computer data transmitted from the first computer through the first firewall via a network connection initiated by the first computer;

determining that the data received from the first computer is intended to be delivered to the second computer; and

transmitting the data to the second computer via the receive channel.

67. (New) The method of claim 66, wherein the request comprises a message transmitted using a secure socket layer (SSL) protocol, a file transfer protocol (FTP), a HyperText Transfer Protocol (HTTP), or an electronic mail protocol.

68. (New) The method of claim 66, wherein the request comprises an HTTP POST message transmitted through the second firewall to port 80 or port 8080.

69. (New) The method of claim 66, wherein the data received from the first computer comprises an HTTP message encrypted using encryption keys shared between the first computer and the second computer, and wherein the third intermediate computer does not decrypt the encrypted HTTP message.

70. (New) The method of claim 66, wherein the data received from the first computer comprises an HTTP message encrypted using encryption keys shared between the first computer and the third intermediate computer, and wherein the third intermediate computer decrypts the HTTP message received from the first computer and re-encrypts the HTTP message using encryption keys shared between the third intermediate computer and the second computer.

71. (New) The method of claim 70, wherein decrypting the HTTP message comprises decrypting encrypted header information, the encrypted header information comprising one or more of an encrypted IP address, an encrypted username of said second computer, an encrypted header length, an encrypted message length, an encrypted application identifier, an encrypted time and date stamp, and an encrypted message type.

72. (New) The method of claim 66, wherein communication between the first computer and the third intermediate computer is initiated by the first computer, and wherein communication between the second computer and the third intermediate computer is initiated by the second computer.

73. (New) The method of claim 66, wherein the first firewall and the second firewall are configured not to allow incoming network messages, unless the incoming network messages are responsive to network messages transmitted by a computer inside the firewall.

74. (New) A method of communicating between a first computer protected by a first firewall and a second computer protected by a different second firewall via a third intermediate computer, comprising the steps of:

transmitting a request from the second computer to the third intermediate computer through the second firewall to establish a receive channel between the third intermediate computer and the second computer;

receiving from the third intermediate computer a response to the request, the response establishing a receive channel between the third intermediate computer and the second computer that is to be kept open for subsequent transmissions from the third intermediate computer; and

receiving data via the receive channel, wherein the data was transmitted from the first computer to the third intermediate computer through the first firewall via a network connection initiated by the first computer, then transmitted from the third intermediate computer to the second computer via the receive channel.

75. (New) The method of claim 74, wherein the request comprises a message transmitted using a secure socket layer (SSL) protocol, a file transfer protocol (FTP), a HyperText Transfer Protocol (HTTP), or an electronic mail protocol.

76. (New) The method of claim 74, wherein the request comprises an HTTP POST message transmitted through the second firewall to port 80 or port 8080.

77. (New) The method of claim 74, wherein the data received via the receive channel comprises an HTTP message from the first computer, the HTTP message encrypted using encryption keys shared between the first computer and the second computer.

78. (New) The method of claim 74, wherein the data received via the receive channel comprises an HTTP message from the first computer, the HTTP message encrypted using encryption keys shared between the third intermediate computer and the second computer

79. (New) The method of claim 78, wherein the encrypted HTTP message comprises encrypted header information including one or more of an encrypted IP address, an encrypted username of said second computer, an encrypted header length, an encrypted message length, an encrypted application identifier, an encrypted time and date stamp, and an encrypted message type.

80. (New) The method of claim 74, wherein communication between the first computer and the third intermediate computer is initiated by the first computer, and wherein communication between the second computer and the third intermediate computer is initiated by the second computer.

81. (New) The method of claim 74, wherein the first firewall and the second firewall are configured not to allow incoming network messages, unless the incoming network messages are responsive to network messages transmitted by a computer inside the firewall.